UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/775,537	02/09/2004	Brian Hernacki	SYMAP041	6706

21912 7590 04/28/2009

VAN PELT, YI & JAMES LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

EXAMINER	
TRAN, TUNG Q	

ART UNIT	PAPER NUMBER
2416	

MAIL DATE	DELIVERY MODE
04/28/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/775,537	HERNACKI, BRIAN	
	Examiner	Art Unit	
	TUNG Q. TRAN	2416	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 February 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5,7-16 and 18-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5,7-16 and 18-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 2/17/2009 has been entered.

Response to Arguments

2. Applicant's arguments with respect to claims 1-5,7-16 and 18-23 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-5, 7, 8, and 18-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pochon et al. (US 2003/0048793), of record, in view of Ahmed et al. (US 2004/0083385) and further in view of Hamadeh et al. (US 2004/0093521).

Pochon discloses method and apparatus for data normalization comprising the following features.

Regarding claims 1, 20, and 21, a method/system/computer readable storage medium comprising computer instructions for assembling fragmented network traffic, comprising: detecting in the fragmented network traffic an anomaly that could result in two or more fragments contained in the fragmented network traffic being reassembled at a monitoring node to obtain a reassembled data flow that is different than a corresponding data as reassembled at a destination node to which the fragmented network traffic is addressed (see [0089]-[0093], esp. [0093], where an NIDS checks to determine whether there is a conflict between previously received fragments and a currently received fragment, i.e. check to determine if there is an anomaly, see also [0022]-[0026]); and performing further processing on the fragmented network traffic having the anomaly (see [0093], where the fragmented network traffic having the anomaly is discarded).

Regarding claims 2 and 18, wherein detecting an anomaly comprises determining that said two or more fragments overlap (see [0022]-[0026).

Regarding claim 3, wherein determining that said two or more fragments overlap comprises reading a header value associated with one of the fragments (see [0091]-[0092]).

Regarding claim 4, wherein the header value comprises an offset value (see [0091]-[0092]).

Regarding claims 5 and 19, wherein detecting an anomaly comprises determining that said two or more fragments overlap and that at least two of said fragments comprise different data for an overlapping portion of said fragments (see [0022]-[0026]).

Pochon disclosed the claimed limitations above. Pochon does not expressly disclose the following features: regarding claims 1, 20, and 21, initiating in response to detecting said anomaly expanded buffering of fragments contained in said fragmented network traffic; and performing a query to determine configuration information associated with how the destination node is configured to reassemble overlapping fragments; regarding claims 7 and 22, querying the destination node; regarding claims 8 and 23, querying an information base.

Ahmed discloses dynamic network security apparatus and methods for network processors comprising the following features.

Regarding claims 1, 20, and 21, initiating in response to detecting said anomaly expanded buffering of packets contained in the packet network traffic (see increasing the size of the connection queue when detecting a TCP SYN attack recited in [0030]); and performing a query to determine configuration information (see processing a query to determine configuration information associated with the communication network recited in [0034-0035]).

Regarding claims 7 and 22, querying the destination node (see [0034-0035]).

Regarding claims 8 and 23, querying a information base (see [0034-0035]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method/system/computer readable storage medium of Pochon by using features, as taught by Ahmed, in order to dynamically load a security algorithm in a network processor based on network conditions (Ahmed: [0001]) and allow a more careful examination of the suspicious packet to determine whether the packet is benign or malicious.

Pochon and Ahmed disclosed the claimed limitations above. They do not explicitly disclose the following features: regarding claims 1, 20, and 21, how the destination node is configured to reassemble overlapping fragments.

Hamadeh discloses real-time packet traceback and associated packet marking strategies comprising the following features.

Regarding claims 1, 20, and 21, determining configuration information associated with how the destination node is configured to reassemble overlapping fragments (see [114-118] and Fig. 7, where configuration information related to reconstruction algorithm the destination is used to reconstruct overlapping fragments is determined to form a set of IP addresses).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method/system/computer readable storage medium of Pochon and Ahmed by using features, as taught by Hamadeh, in order to be able to determine the source of an attack within few minutes of its launch and while the attack is still ongoing. Hence, the reconstruction for traceback provides real-time identification of the addresses of routers involved in the attack.

5. Claims 9-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pochon et al. (US 2003/0048793), of record, in view of Ahmed et al. (US 2004/0083385) and further in view of Hamadeh et al. (US 2004/0093521) and Cantrell et al. (US 2004/0093513).

Pochon, Ahmed, and Hamadeh disclosed the claimed limitations above. Pochon also discloses the following features.

Regarding claim 9, performing further processing comprises reassembling the fragmented network traffic (see [0039]-[0040]).

They do not explicitly disclose the following features: regarding claim 9, generating more than one variant of the reassembled data flow;

Cantrell discloses active network defense system and method comprising the following features.

Regarding claim 9, generating more than one variant of the reassembled data flow (see [0026] and [0062]-[0065]).

Regarding claim 10, processing the anomaly to determine whether the fragmented network traffic is associated with a threat (see [0065]).

Regarding claim 11, performing an action on the fragmented network traffic based on whether the fragmented network traffic is associated with a threat (see [0063]).

Regarding claim 12, discarding at least a portion of the fragmented network traffic if the fragmented network traffic is associated with a threat (see [0063]).

Regarding claim 13, copying one or more fragments comprising the fragmented network traffic to a buffer (see [0065], where it is implicit that the traffic is copied to a buffer).

Regarding claim 14, performing further processing comprises sending an alert (see [0063]).

Regarding claim 15, performing further processing comprises determining whether the fragmented network traffic should be blocked (see [0063]).

Regarding claim 16, performing further processing comprises determining whether the fragmented network traffic should be forwarded to the destination node (see [0063]).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method/system/computer readable storage medium of Pochon, Ahmed, and Hamadeh by using features, as taught by Cantrell, in order to monitor and block traffic in an automated fashion, identify threats existing across multiple sessions and within individual sessions, block threatening packet traffic and terminate threatening sessions, extract suspicious traffic from the data flow for further examination with more comprehensive content matching as well as asset risk analysis, and provide a flow control mechanism to control passage rate for packets passing through the data flow. See the abstract.

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to TUNG Q. TRAN whose telephone number is (571)272-9737. The examiner can normally be reached on Mon-Fri: 7:30 am - 5 pm, off alternative Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kwang B. Yao can be reached on (571) 272-3182. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/T. Q. T./
Examiner, Art Unit 2416

/Kwang B. Yao/

Supervisory Patent Examiner, Art Unit 2416